ABSTRACT OF THE DISCLOSURE

A computer system processor incorporates a special S- latch which may only be set by secure signals. One state of the S-latch sets the processor into a secure mode where it only executes instructions and not commands from an In Circuit Emulator (ICE) unit. A second state of the S-latch sets the processor into a non-secure mode. A non-volatile random access memory (NVRAM) is written with secure data which can only be read by boot block code stored in a BIOS storage device. The boot block code is operable to read the secure data in the NVRAM and set the S-latch to an appropriate security state. If the boot block code cannot set the S-latch, then remaining boot up with BIOS data is stopped. On boot up the boot block code reads the NVRAM and sets the S-latch into the appropriate security state.

A:\patent.wpd
1097:7036/P164US